UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/802,048	03/17/2004	Takio Yamashita	67471-037	3476

7590 09/17/2008

MCDERMOTT, WILL & EMERY
600 13th Street, N.W.
Washington, DC 20005-3096

EXAMINER	
TABOR, AMARE F	
ART UNIT	PAPER NUMBER
2139	
MAIL DATE	DELIVERY MODE
09/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/802,048	YAMASHITA, TAKIO	
	Examiner	Art Unit	
	AMARE TABOR	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 March 2008* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *07/28/2008 & 11/29/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. **Claims 1-18** are examined.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 13 and 18 are rejected under 35 U.S.C. 102(b) as being anticipated by "Sedlak" (US 6,182,217 B1)

As per Claim 13, Sedlak teaches,

A host computer which (i) is connected to a microprocessor operable to store secret program information and (ii) debugs the program information in the microprocessor [see FIGS.1 and 2], comprising: a receiving unit operable to receive key information from a user [see receiving unit **T** in FIG.1]; a sending unit operable to store the received key information therein [see **SW** and **SWL** in FIG.1] and send the received key information to the microprocessor [see for example, col.5, lines 25-27]; and a transmission unit operable to securely perform transmission of program information [see **SE** and **V** in FIG.1] with the microprocessor using the key information stored in the sending unit [see for example, col.5, lines 46-57].

As per Claim 18, Sedlak teaches,

A read/write device that is connected to a microprocessor operable to store secret program information [see FIGS.1 and 2], comprising: a receiving unit operable to receive key information from a user [see **T** in FIG.1]; a sending unit operable to store the received key information therein [see **SW** and

SWL in FIG.1] and send the received key information to the microprocessor [see for example, col.5, lines 25-27]; and a transmission unit operable to securely perform transmission of program information [see **SE** and **V** in FIG.1] with the microprocessor using the key information [see for example, col.5, lines 46-57].

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-12 and 14-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Sedlak" in view of Foster et al. (US 2003/0200454 A1 – "Foster")

As per Claim 1, Sedlak teaches,

A debug system comprising: a microprocessor [see **CPU** in FIGS.1 and 2] operable to store secret program information [see for example, col.5, lines 35-38]; and a host computer [see **LG** in FIG.1] that is connected to the microprocessor so as to debug the program information in the microprocessor [*Sedlak discloses **LG is connected to the CPU***],

wherein the microprocessor includes: a nonvolatile memory [see **ROM** and **EEPROM** in FIG.1] which (i) has an area for storing key [see **KEY 1** and **KEY 2** in FIG.1] information that is used to securely handle program information [see for example, col.5, lines 43-45] and (ii) is writable only once [see for example, col.3, lines 53-60 and col.4, lines 9-17 – *where **Sedlak** discloses that register and keyword are erased when the data processing device is switched off*]; and a first transmission unit operable to securely perform transmission of program information with the host computer [see **VE** in FIG.1] using the key information that has been written into the nonvolatile memory [see for example, col.5, lines 43-61], the key information that has been written into the nonvolatile memory is not readable outside of the

microprocessor [see for example, 6, lines 8-20 – *where **Sedlak** discloses encoding technique so that the keys would not be readable from outside*], and

the host computer includes: a receiving unit operable to receive key information from a user [see **T** in FIG.1]; a sending unit operable to store therein the key information received from the user and send the key information [see **SW** and **SWL** in FIG.1] to the microprocessor [see for example, col.5, lines 25-27]; and a second transmission unit operable to securely perform transmission of program information [see **SE** and **V** in FIG.1] with the microprocessor using the key information stored in the sending unit [see for example, col.5, lines 46-57].

Sedlak discloses key stored in nonvolatile memory [see FIG.1 – *where **Sedlak** disclose **KEY 1** and **KEY 2** stored in **ROM** and **EEPROM***] and writing unit [see **T** in FIG.1]; but fails to disclose if no key information is stored in the nonvolatile memory, receive key information from the host computer and write the key information into the nonvolatile memory. However, in the same field of endeavor, **Foster** discloses receiving key information from the host computer and write the key information into the nonvolatile memory if no key information is stored in the nonvolatile memory [see FIGS.6 and 13; and for example, par.0068-0071 and 0090-0093]. Therefore, it would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention was made, to modify the system of **Sedlak** by incorporating the teaching of **Foster** in order to recover integrated system functionality following a trigger event, such as tampering [see at least abstract of **Foster**].

As per Claim 2, Sedlak-Foster combination teaches,

A microprocessor which is operable to store secret program information and is connected to a host computer that is used to debug the program information in the microprocessor, comprising: a program information storing unit operable to store the program information which is one of a program, data and a program and data [see **CPU** in FIGS.1 and 2; and for example, col.5, lines 35-38 of **Sedlak**]; an executing unit operable to read the program information to perform an operation corresponding to the read program information [see **LG** in FIG.1 of **Sedlak**]; a nonvolatile memory [see **ROM** and **EEPROM** in

FIG.1 of **Sedlak**] which (a) has an area for storing key information that is used to securely handle program information [see **KEY 1** and **KEY 2** in FIG.1 of **Sedlak**] and (b) is writable only once [see for example, col.3, lines 53-60 and col.4, lines 9-17 of **Sedlak**];

a writing unit [see **T** in FIG.1 of **Sedlak**] operable to, if no key information is stored in the nonvolatile memory, receive key information from the host computer and write the received key information into the nonvolatile memory [see FIGS.6 and 13; and for example, par.0068-0071 and 0090-0093 of **Foster**]; and

a transmission unit operable to securely perform transmission of program information with the host computer using the key information that has been written into the nonvolatile memory [see **VE** in FIG.1; and see for example, col.5, lines 43-61 of **Sedlak**], wherein the key information that has been written into the nonvolatile memory is not readable outside of the microprocessor [see for example, 6, lines 8-20 of **Sedlak**].

As per Claim 3, Sedlak-Foster combination teaches,

wherein the nonvolatile memory additionally stores therein flag information that indicates whether key information is stored in the nonvolatile memory, the transmission unit reads the flag information [see FIG.5 – *where **Foster** discloses **KEY SETS, ADDRESS TABLE**, …*See also **INTEGRITY CHECK (OPTIONAL) 245** in FIG.7A-B of **Foster**], and if the read flag information indicates that no key information is stored in the nonvolatile memory, the writing unit receives the key information from the host computer, and writes the key information received from the host computer into the nonvolatile memory [see FIGS.6 and 13; and for example, par.0068-0071 and 0090-0093 of **Foster**].

As per Claim 4, Sedlak-Foster combination teaches,

wherein the transmission unit includes: an encryption unit operable to encrypt the program information stored in the program information storing unit using the key information that has been stored in the nonvolatile memory [see **VE** in FIG.1 of **Sedlak**]; and an output unit operable to output the encrypted program information [see **BUS** in FIG.1 of **Sedlak**].

As per Claim 5, Sedlak-Foster combination teaches,

wherein the transmission unit further includes an inhibition unit operable to, in response to a request from the host computer, inhibit the output unit from outputting the encrypted program information [see **SW** and **SWL** in FIG.1 of **Sedlak**].

As per Claim 6, Sedlak-Foster combination teaches,

wherein the transmission unit further includes: an inhibition condition storing unit storing an inhibition condition that relates to the key information received from the host computer [see FIG.5 of **Foster**]; and an inhibition unit operable to, if the key information received from the host computer satisfies the inhibition condition, inhibit the output unit from outputting the encrypted program information [see **SE** and **V** in FIG.1 of **Sedlak**].

As per Claim 7, Sedlak-Foster combination teaches,

wherein the program information stored in the program information storing unit is encrypted program information which is one of an encrypted program, encrypted data, and an encrypted program and encrypted data [see **ENCRYPTION DECRYPTION 249** in FIG..2 of **Foster**], the executing unit (i) reads the key information that has been stored in the nonvolatile memory [see **VOLITILE MEMORY 280** in FIG.2 of **Foster**], (ii) decrypts the encrypted program information using the read key information so as to generate decrypted program information which is one of a decrypted program, decrypted data, and a decrypted program and decrypted data [see **ENCRYPTION DECRYPTION 249** in FIG..2 of **Foster**], and (iii) performs an operation corresponding to the decrypted program information, wherein the transmission performed by the transmission unit is transmission of encrypted program information [see **249** sending **BOOT CODE ENCRYPTED WITH MASTER KEY SET** to the **VOLITILE MEMORY** in FIG.7A-B of **Foster**].

As per Claim 8, Sedlak-Foster combination teaches,

wherein the executing unit encrypts a result of the operation using the key information that has been stored in the non-volatile memory [see **VE** in FIG.1 of **Sedlak**], and writes the encrypted result into the program information storing unit [see the Registers **R1, R2,…** in FIG.2 of **Sedlak**].

As per Claim 9, Sedlak-Foster combination teaches,

wherein the program stored in the program information storing unit is an encrypted program, and the program information storing unit has a path to communicate with an external device [see **BUS** in FIGS.1 and 2 of **Sedlak**].

As per Claim 10, Sedlak-Foster combination teaches,

wherein the key information that has been written into the non-volatile memory is constituted by one or more pieces of partial key information [see **SECRET KEY SETS** in FIG.5 of **Foster**], the program stored in the program information storing unit is a plurality of encrypted partial programs each of which corresponds to any of the pieces of partial key information, and the executing unit (a) reads a piece of partial key information from the nonvolatile memory, (b) reads one or more of the encrypted partial programs corresponding to the read piece of partial key information, from the program information storing unit, (c) decrypts the read encrypted partial programs using the read piece of partial key information to generate decrypted partial programs, and (d) performs an operation corresponding to the decrypted partial programs [see FIGS.12A-C; and for example, par.0089 – *where **Foster** discloses storing, reading, encrypting and decrypting data in cache data blocks*].

As per Claim 11, Sedlak-Foster combination teaches,

further including a cache memory [see **INSTRUCTION CACHE 900 and DATA CACHE 910** in FIGS.9 and 12A-C; and for example, par.0089 of **Foster**], wherein the program information stored in the program information storing unit is encrypted program information which is one of an encrypted program, encrypted data, and an encrypted program and encrypted data [see **ENCRYPTION DECRYPTION 249** in FIG..2 of **Foster**], the executing unit (a) reads the key information that has been stored in the non-volatile

memory, (b)decrypts the encrypted program information using the read key information so as to generate decrypted program information which is one of a decrypted program, decrypted data and a decrypted program and decrypted data [see **ENCRYPTION DECRYPTION 249** in FIGS.12A-C of **Foster**], (c) writes the decrypted program information into the cache memory [see **PROCESSOR READS ENCRYPTED DATA AND DECRYPTS IT IN SOFTWARE USING SECURE CODE** in FIG.12B of **Foster**], (d) reads the decrypted program information from the cache memory in accordance with a processing speed of the executing unit [see FIG.9 – *where **Foster** discloses **RETURN SECURE CODE** from **ENCRYPTION DECRYPTION 249***], and (e) performs an operation corresponding to the decrypted program information, and the transmission performed by the transmission unit is transmission of encrypted program information [see **249** sending **BOOT CODE ENCRYPTED WITH MASTER KEY SET** to the **VOLITILE MEMORY** in FIG.7A-B of **Foster**].

As per Claim 12, Sedlak-Foster combination teaches,

wherein the nonvolatile memory additionally stores flag information indicating whether the key information is stored in the nonvolatile memory, the transmission unit reads the flag information, if the read flag information indicates that no key information is stored in the nonvolatile memory [see FIG.5 – *where **Foster** discloses **KEY SETS, ADDRESS TABLE**, …* See also **INTEGRITY CHECK (OPTIONAL) 245** in FIG.7A-B of **Foster**], the transmission unit reads the program information from the program information storing unit and outputs the read program information to the host computer, and if the read flag information indicates that the key information has been stored the nonvolatile memory, the transmission unit reads the program information from the program information storing unit, encrypts the read program information using the key information that has been stored in the nonvolatile memory, and outputs the encrypted program information to the host computer [see FIGS.6 and 13; and for example, par.0068-0071 and 0090-0093 of **Foster**].

As per Claim 14, Sedlak teaches,

wherein the transmission unit includes: a program information receiving unit operable to receive, from the microprocessor [see FIG.1], encrypted program information which has been generated by encrypting the program information; and a decrypting unit operable to decrypt the encrypted program information using the key information stored in the sending unit so as to generate decrypted program information [see **CPU and VE** in FIGS. 1 and 2].

Sedlak discloses transmitting decrypted data [see FIGS.1 and 2]; but fails to disclose a display unit operable to display the decrypted program information generated by the decrypting unit; however, **Foster** discloses a displaying the decrypted program information generated by the decrypting unit [see FIGS.12A-C]. Therefore, it would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention was made, to modify the system of **Sedlak** by incorporating the teaching of **Foster** in order write a clear data blocks in the external memory [see at least par.0089 of **Foster**].

As per Claim 15, Sedlak-Foster combination teaches,

wherein the transmission unit further includes: a program information input unit operable to receive, from the user, program information which is one of a program, data and a program and data [see **T** in FIG.1 of **Sedlak**]; an encrypting unit operable to encrypt the program information received from the user, using the key information stored in the sending unit so as to generate encrypted program information [see **CPU and VE** in FIGS. 1 and 2 of **Sedlak**]; and an output unit operable to output the encrypted program information generated by the encrypting unit to the microprocessor [see FIGS.12A-C of **Foster**].

As per Claim 16, Sedlak-Foster combination teaches,

a storage unit storing a source program [see **PERSISTENT STORAGE 243** in FIG.7A-B of **Foster**]; a conversion unit operable to convert the source program into an object program [see **PROCESSOR 210** in FIG.7A-B of **Foster**]; and an encrypting unit operable to encrypt the object program using the key information stored in the sending unit so as to generate an encrypted program [see

ENCRYPTION DECRYPTION 249 in FIG.7A-B of **Foster**], wherein the transmission unit transmits the encrypted program generated by the encrypting unit to the microprocessor [see **249** sending **BOOT CODE ENCRYPTED WITH MASTER KEY SET** to the **VOLITILE MEMORY** in FIG.7A-B of **Foster**].

As per Claim 17, Sedlak-Foster combination teaches,

wherein the transmission unit further includes: an inhibition condition storing unit storing an inhibition condition that relates to the key information [see FIG.5 of **Foster**]; and an inhibition request output unit operable to, if the key information satisfies the inhibition condition, output a request, to the microprocessor, to inhibit the transmission of the encrypted program information [see **SE** and **V** in FIG.1 of **Sedlak**].

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-892).

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to AMARE TABOR whose telephone number is (571)270-3155. The examiner can normally be reached on Mon-Fri 8:00a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Amare Tabor
(AU 2139)

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139